CERT Advisory CA-1991-15 Mac/PC NCSA Telnet Vulnerability

Original issue date: September 10, 1991
Last revised: September 18, 1997
Attached copyright statement

A complete revision history is at the end of this file.

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received information concerning a vulnerability in the default configurations of National Center for Supercomputing Applications (NCSA) Telnet for both the Macintosh and the PC. The vulnerability also affects the version of NCSA Telnet with IBM 3270 terminal emulation distributed by Clarkson University. Two workarounds are available that correct this problem.

NCSA has committed to changing the default configurations in future releases. Maintenance updates for both the Macintosh and the PC are planned to be released in about 2 months.

NCSA provides two e-mail addresses for Telnet questions, comments, and bug reports:

PC Telnet pctelnet@ncsa.uiuc.edu

Mac Telnet mactelnet@ncsa.uiuc.edu

I. Description

The default configuration of NCSA Telnet for both the Macintosh and the PC has a serious vulnerability in its implementation of an ftp server.

The default configuration file enables ftp via the "ftp=yes" line. However, sites should be aware that ftp is also enabled in the absence of any ftp statement in the configuration file.

II. Impact

Any Internet user can connect via ftp to a PC or Macintosh running the default configuration of NCSA Telnet and gain unauthorized read and write access to any of its files, including system files.

III. Solution

Either disable ftp server functionality or provide password protection as described below.

To disable the ftp server, add an "ftp=no" line in the configuration file.

If the ftp server option is enabled (via either an "ftp=yes" line in the configuration file or the absence of an ftp statement in the configuration file), then the Telpass program (included with both Mac and PC versions) can be used to provide password protection. Telpass is used to enter usernames and encrypted passwords into a password file. The configuration file specifies the name and location of the password file in the "passfile=" statement. The usage of Telpass is documented in Chapter 5 of version 2.4 of the Macintosh version documentation and Chapter 7 of version 2.3 of the PC version. Note that the documentation (as well as the package itself) is available by anonymous ftp from ftp.ncsa.uiuc.edu (141.142.20.50).

The instructions for enabling password protection differ between the Macintosh and PC versions, but in both cases they involve enabling the "passfile" option in the configuration file, and creating usernames and encrypted passwords with the Telpass program.

CERT/CC strongly urges all sites running NCSA Telnet to implement one of these two workarounds.

The CERT/CC would like to thank NCSA and Clarkson University for their assistance.

Revision History

```
September 18,1997  Attached Copyright Statement
```